

Ds-bounds for cyclic codes: New bounds for abelian codes.

J.J. Bernal, M. Guerreiro* and J. J. Simón[†]

April 12, 2016

Abstract

In this paper we develop a technique to extend any bound for cyclic codes constructed from its defining sets (ds-bounds) to abelian (or multivariate) codes. We use this technique to improve the searching of new bounds for abelian codes.

Keywords: Abelian code, bounds for minimum distance, cyclic codes, algorithm.

1 Introduction

The study of abelian codes is an important topic in Coding Theory, having an extensive literature, because they have special algebraic properties that allow one to construct good codes with efficient encoding and decoding algorithms. More precisely, regarding decoding, the two most known general techniques are permutation decoding [1] and the so called locator decoding [4] that uses the Berlekamp-Massey algorithm [17] (see also [11]).

Even though the mentioned decoding methods require to know the minimum distance, or a bound for it, there are not much literature or studies on its computation and properties, or it does exist only for specific families of codes (see [4]). Concerning BCH bound, in [6], Camion introduces an extension from cyclic to abelian codes which is computed through the apparent distance of such codes. Since then there have been some papers improving the original computation and giving a notion of multivariate BCH bound and codes (see [2, 16]).

These advances lead us to some natural questions about the extension to the multivariate case of all generalizations and improvements of the BCH bound

*M. Guerreiro is with Departamento de Matemática, Universidade Federal de Viçosa, 36570-900 Viçosa-MG, Brazil. Supported by CNPq-Brazil. E-mail: marines@ufv.br

[†]J. J. Bernal and J. J. Simón are with the Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain. Partially supported by MINECO project MTM2012-35240 and Fundación Séneca of Murcia. E-mail: {josejoaquin.bernal, jsimon}@um.es

known for cyclic codes; specifically, those bounds on the minimum distance for cyclic codes from defining sets.

There are dozens of papers on this topic regarding approaches from matrix methods ([3, 21]) through split codes techniques ([8, 12]) until arriving at the most classic generalizations based on computations over the defining set, as the HT bound [9], the Ross bound [15] and the improvements by Van Lint and Wilson [18].

Having so many references on the subject, it seems very necessary to find a general method that allows us to extend any bound for the minimum distance of cyclic codes based on the defining set to the multivariate case. This is our goal. We shall show a method to extend to the multivariate case any bound of the type mentioned via associating an apparent distance to such bound.

To do this, we give in Section 3 a notion of general defining set bound (ds-bound) for the minimum distance of cyclic codes; then, in Section 4 we relate the weight of codewords with the apparent distance of their discrete Fourier transforms. In Section 5, we use this technique to define the apparent distance of an abelian code with respect to a set of ds-bounds. In Section 6, we show an algorithm (of linear complexity by Remark 21) to compute this apparent distance. Finally, we show how one may improve the searching of new bounds for abelian codes.

2 Preliminaries

Let \mathbb{F}_q be a finite field with q elements, with q a power of a prime p , r_i be positive integers, for all $i \in \{1, \dots, s\}$, and $n = r_1 \cdots r_s$. We denote by \mathbb{Z}_{r_i} the ring of integers modulo r_i and we shall always write its elements as canonical representatives.

An **abelian code** of length n is an ideal in the algebra $\mathbb{F}_q(r_1, \dots, r_s) = \mathbb{F}_q[X_1, \dots, X_s]/(X_1^{r_1} - 1, \dots, X_s^{r_s} - 1)$ and throughout the work we assume that this algebra is semisimple; that is, $\gcd(r_i, q) = 1$, for all $i \in \{1, \dots, s\}$. Abelian codes are also called multidimensional cyclic codes (see, for example, [10]).

The codewords are identified with polynomials $f(X_1, \dots, X_s)$ in which, for each monomial, the degree of the indeterminate X_k belongs to \mathbb{Z}_{r_k} . We denote by I the set $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ and we write the elements $f \in \mathbb{F}_q(r_1, \dots, r_s)$ as $f = f(X_1, \dots, X_s) = \sum a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, where $\mathbf{i} = (i_1, \dots, i_s) \in I$ and $\mathbf{X}^{\mathbf{i}} = X_1^{i_1} \cdots X_s^{i_s}$. Given a polynomial $f \in \mathbb{F}_q[X_1, \dots, X_s]$ we denote by \bar{f} its image under the canonical projection onto $\mathbb{F}_q(r_1, \dots, r_s)$.

For each $i \in \{1, \dots, s\}$, we denote by R_{r_i} (resp., U_{r_i}) the set of all r_i -th roots of unity (resp. all r_i -th primitive roots of unity) and define $R = \prod_{i=1}^s R_{r_i}$ and $U = \prod_{i=1}^s U_{r_i}$.

For $f = f(X_1, \dots, X_s) \in \mathbb{F}_q[X_1, \dots, X_s]$ and $\bar{\alpha} \in R$, we write $f(\bar{\alpha}) = f(\alpha_1, \dots, \alpha_s)$. For $\mathbf{i} = (i_1, \dots, i_s) \in I$, we write $\bar{\alpha}^{\mathbf{i}} = (\alpha_1^{i_1}, \dots, \alpha_s^{i_s})$.

It is a known fact that every abelian code C in $\mathbb{F}_q(r_1, \dots, r_s)$ is totally determined by its **root set** or **set of zeros**

$$Z(C) = \{\bar{\alpha} \in R \mid f(\bar{\alpha}) = 0, \text{ for all } f \in C\}.$$

The set of non zeros is denoted by $\overline{Z(C)} = \mathbb{Z}_n \setminus Z(C)$. For a fixed $\bar{\alpha} \in U$, the code C is determined by its **defining set**, with respect to α , which is defined as

$$\mathcal{D}_{\bar{\alpha}}(C) = \{\mathbf{i} = (i_1, \dots, i_s) \in I \mid f(\bar{\alpha}^{\mathbf{i}}) = 0, \text{ for all } f \in C\}.$$

Given an element $a = (a_1, \dots, a_s) \in I$, we shall define its **q -orbit** modulo (r_1, \dots, r_s) as $Q(a) = \{(a_1 \cdot q^i, \dots, a_s \cdot q^i) \in I \mid i \in \mathbb{N}\}$. In our case, it is known that the defining set $\mathcal{D}_{\bar{\alpha}}(C)$ is a disjoint union of q -orbits modulo (r_1, \dots, r_s) . Conversely, every union of q -orbits modulo (r_1, \dots, r_s) determines an abelian code (an ideal) in $\mathbb{F}_q(r_1, \dots, r_s)$ (see, for example, [2] for details). We recall that the notions of root set and defining set also apply to polynomials. Moreover, if C is the ideal generated by the polynomial f in $\mathbb{F}_q(r_1, \dots, r_n)$, then $\mathcal{D}_{\bar{\alpha}}(C) = \mathcal{D}_{\bar{\alpha}}(f)$.

We recall that the notion of defining set also applies to cyclic codes. For $s = 1$ and $r_1 = n$, a q -orbit is called a **q -cyclotomic coset** of a positive integer b modulo n and it is the set $C_q(b) = \{b \cdot q^i \in \mathbb{Z}_n \mid i \in \mathbb{N}\}$.

Let $\mathbb{L}|\mathbb{F}_q$ be an extension field containing U_{r_i} , for all $i \in \{1, \dots, s\}$. The **discrete Fourier transform of a polynomial** $f \in \mathbb{F}_q(r_1, \dots, r_s)$ **with respect to** $\bar{\alpha} \in U$ (also called Mattson-Solomon polynomial in [16]) is the polynomial $\varphi_{\bar{\alpha}, f}(\mathbf{X}) = \sum_{\mathbf{j} \in I} f(\bar{\alpha}^{\mathbf{j}}) \mathbf{X}^{\mathbf{j}} \in \mathbb{L}(r_1, \dots, r_s)$. It is known that the discrete Fourier transform may be viewed as an isomorphism of algebras $\varphi_{\bar{\alpha}} : \mathbb{L}(r_1, \dots, r_s) \longrightarrow (\mathbb{L}^{|I|}, \star)$, where the multiplication “ \star ” in $\mathbb{L}^{|I|}$ is defined coordinatewise. Thus, we may see $\varphi_{\bar{\alpha}, f}$ as a vector in $\mathbb{L}^{|I|}$ or as a polynomial in $\mathbb{L}(r_1, \dots, r_s)$ (see [6, Section 2.2]).

3 Defining set bounds for cyclic codes

In this section we deal with cyclic codes; that is $r_1 = n$. By $\mathcal{P}(\mathbb{Z}_n)$ we denote the set of the parts of \mathbb{Z}_n . We take an arbitrary $\alpha \in U_n$.

Definition 1 *A **defining set bound** (or **ds-bound**, for short) for the minimum distance of cyclic codes is a family of relations $\delta = \{\delta_n\}_{n \in \mathbb{N}}$ such that, for each $n \in \mathbb{N}$, $\delta_n \subseteq \mathcal{P}(\mathbb{Z}_n) \times \mathbb{N}$ satisfies the following conditions:*

1. *If C is a cyclic code in $\mathbb{F}(n)$ such that $\emptyset \neq N \subseteq \mathcal{D}_{\alpha}(C)$, then $1 \leq a \leq d(C)$, for all $(N, a) \in \delta_n$.*
2. *If $\emptyset \neq N \subseteq M$ are subsets of \mathbb{Z}_n then $(N, a) \in \delta_n$ implies $(M, a) \in \delta_n$.*
3. *For all $N \in \mathcal{P}(\mathbb{Z}_n)$, $(N, 1) \in \delta_n$.*

From now on, sometimes we write simply δ to denote a ds-bound or any of its elements independently on the length of the code. It will be clear in the context which one is being used.

Remarks 2 (1) For example, the BCH bound states that for any cyclic code in $\mathbb{F}_q(n)$ that has a string of $t - 1$ consecutive powers of some $\alpha \in U_n$, the minimum distance of the code is at least t [13, Theorem 7.8].

Now, define $\delta \subset \mathcal{P}(\mathbb{Z}_n) \times \mathbb{N}$ as follows: for any $a \geq 2$, $(N, a) \in \delta$ if and only if there exist i_0, i_1, \dots, i_{a-2} in N which are consecutive integers modulo n . Then the BCH bound says that δ is a ds-bound, for any cyclic code (we only have to state Condition 3 as a convention).

(2) It is easy to check that all extensions of the BCH bound, all new bounds from the defining set of a cyclic code as in [3, 9, 14, 15, 21] and the new bounds and improvements arising from Corollary 1, Theorem 5 and results in Section 4 and Section 5 in [18], also verify Definition 1.

In order to relate the idea of ds-bound with the Camion's apparent distance, which will be defined later, we consider the following family of maps.

Definition 3 Let δ be a ds-bound for the minimum distance of cyclic codes. The **optimal ds-bound associated to** δ is the family $\bar{\delta} = \{\bar{\delta}_n\}_{n \in \mathbb{N}}$ of maps $\bar{\delta}_n : \mathcal{P}(\mathbb{Z}_n) \rightarrow \mathbb{N}$ defined as $\bar{\delta}_n(N) = \max\{b \in \mathbb{N} \mid (N, b) \in \delta_n\}$.

The following result is immediate.

Lemma 4 Let δ be a ds-bound for the minimum distance of cyclic codes. Then, for each $n \in \mathbb{Z}$:

1. If C is a cyclic code in $\mathbb{F}(n)$ such that $\emptyset \neq N \subseteq \mathcal{D}_\alpha(C)$, then $1 \leq \bar{\delta}_n(N) \leq d(C)$.
2. If $\emptyset \neq N \subseteq M \subseteq \mathbb{Z}_n$, then $\bar{\delta}_n(N) \leq \bar{\delta}_n(M)$. ■

As we noted above, we may omit the index of the map $\bar{\delta}_n$, because it will be clear on the context for which value it is being taken.

4 Apparent distance of matrices

We begin this section recalling the notion and notation of a hypermatrix that will be used hereby, as it is described in [2]. For any $\mathbf{i} \in I$, we write its k -th coordinate as $\mathbf{i}(k)$. A **hypermatrix with entries in a set R indexed by I (or an I -hypermatrix over R)** is an s -dimensional I -array, denoted by $M = (a_{\mathbf{i}})_{\mathbf{i} \in I}$, with $a_{\mathbf{i}} \in R$ [19]. The set of indices, the dimension and the ground field will be omitted if they are clear in the context. For $s = 2$, M is a matrix and when $s = 1$, M is a vector. We write $M = 0$ when all its entries are 0 and $M \neq 0$, otherwise. As usual, a **hypercolumn** is defined as

$H_M(j, k) = \{a_{\mathbf{i}} \in M \mid \mathbf{i}(j) = k\}$, with $1 \leq j \leq s$ and $0 \leq k < r_j$, where $a_{\mathbf{i}} \in M$ means that $a_{\mathbf{i}}$ is an entry of M . A hypercolumn will be seen as an $(s - 1)$ -dimensional hypermatrix. In the case $s = 2$, we refer to hypercolumns as rows or columns and, when $s = 1$, we say entries.

Let $D \subseteq I$. The **hypermatrix afforded by** D is defined as $M = (a_{\mathbf{i}})_{\mathbf{i} \in I}$, where $a_{\mathbf{i}} = 1$ if $\mathbf{i} \notin D$ and $a_{\mathbf{i}} = 0$, otherwise. When D is an union of q -orbits we say that M is a **q -orbits hypermatrix**, and it will be denoted by $M = M(D)$. For any I -hypermatrix M with entries in a ring, we define the support of M as the set $\text{supp}(M) = \{\mathbf{i} \in I \mid a_{\mathbf{i}} \neq 0\}$. Its complement with respect to I will be denoted by $\mathcal{D}(M)$. To define and compute the apparent distance of an abelian code we will use the hypermatrix afforded by its defining set, with respect to $\bar{\alpha} \in U$.

We define a partial ordering over the set $\{M(D) \mid D \text{ is union of } q\text{-orbits of } I\}$ of hypermatrices as follows:

$$M(D) \leq M(D') \Leftrightarrow \text{supp}(M(D)) \subseteq \text{supp}(M(D')). \quad (1)$$

Clearly, this condition is equivalent to $D' \subseteq D$. We begin with the apparent distance of a vector in \mathbb{L}^n .

Definition 5 Let δ be a ds -bound for the minimum distance of cyclic codes and $v \in \mathbb{L}^n$ a vector. The **apparent distance of v with respect to δ** (or **δ -apparent distance of v** , for short), denoted by $\delta^*(v)$, is defined as

1. If $v = 0$, then $\delta^*(v) = 0$.
2. If $v \neq 0$, then $\delta^*(v) = \bar{\delta}(\mathbb{Z}_n \setminus \text{supp}(v))$.

From now on we denote by \mathbb{B} a set of ds -bounds that are used to proceed a computation of the apparent distances of matrices, hypermatrices or abelian codes.

Definition 6 Let $v \in \mathbb{L}^n$. The **apparent distance of v with respect to \mathbb{B}** denoted by $\Delta_{\mathbb{B}}(v)$, is:

1. If $v = 0$, then $\Delta_{\mathbb{B}}(v) = 0$.
2. If $v \neq 0$, then $\Delta_{\mathbb{B}}(v) = \max\{\delta^*(v) \mid \delta \in \mathbb{B}\}$.

Remarks 7 The following properties arise straightforward from the definition above, for any $v \in \mathbb{L}^n$.

1. If $v \neq 0$ then $\Delta_{\mathbb{B}}(v) \geq 1$.
2. If $\text{supp}(v) \subseteq \text{supp}(w)$ then $\Delta_{\mathbb{B}}(v) \geq \Delta_{\mathbb{B}}(w)$.

Proposition 8 *Let $f \in \mathbb{L}(n)$ and v be the vector of its coefficients. Fix any $\alpha \in U_n$. Then $\Delta_{\mathbb{B}}(v) \leq \omega(\varphi_{\alpha,f}^{-1})$.*

Proof. Set $N = \mathbb{Z}_n \setminus \text{supp}(v)$ and let C be the abelian code generated by $\varphi_{\alpha,f}^{-1}$ in $\mathbb{L}(n)$. Then $d(C) \leq \omega(\varphi_{\alpha,f}^{-1})$. By properties of the discrete Fourier transform we have $N = \mathcal{D}_{\bar{\alpha}}(\varphi_{\alpha,f}^{-1}) = \mathcal{D}_{\bar{\alpha}}(C)$ and then, by Lemma 4 and the definition of apparent distance, $\Delta_{\mathbb{B}}(v) \leq d(C)$. This gives the desired inequality. ■

Now we define the apparent distance of matrices and hypermatrices with respect to a set \mathbb{B} of ds-bounds.

Definition 9 *Let M be an s -dimensional I -hypermatrix over a field \mathbb{L} . The **apparent distance of M with respect to \mathbb{B}** , denoted by $\Delta_{\mathbb{B}}(M)$, is defined as follows:*

1. $\Delta_{\mathbb{B}}(0) = 0$ and, for $s = 1$, Definition 6 applies.
2. For $s = 2$ and a nonzero matrix M , note that $H_M(1, i)$ is the i -th row and $H_M(2, j)$ is the j -th column of M . Define the **row support of M** as $\text{supp}_1(M) = \{i \in \{0, \dots, r_1 - 1\} \mid H_M(1, i) \neq 0\}$ and the **column support of M** as $\text{supp}_2(M) = \{j \in \{0, \dots, r_2 - 1\} \mid H_M(2, j) \neq 0\}$.

Then put

$$\begin{aligned} \omega_2(M) &= \max\{\bar{\delta}(\mathbb{Z}_{r_2} \setminus \text{supp}_2(M)) \mid \delta \in \mathbb{B}\}, \\ \epsilon_2(M) &= \max\{\Delta_{\mathbb{B}}(H_M(2, j)) \mid j \in \text{supp}_2(M)\} \end{aligned}$$

and set $\Delta_2(M) = \omega_2(M) \cdot \epsilon_2(M)$.

Analogously, we compute the apparent distance $\Delta_1(M)$ for the other variable and finally we define the **apparent distance of M with respect to \mathbb{B}** by

$$\Delta_{\mathbb{B}}(M) = \max\{\Delta_1(M), \Delta_2(M)\}.$$

3. For $s > 2$, proceed as follows: suppose that one knows how to compute the apparent distance $\Delta_{\mathbb{B}}(N)$, for all non zero hypermatrices of dimension $s - 1$. Then first compute the “hypermatrix support” of $M \neq 0$ with respect to the j -th hypercolumn, that is, $\text{supp}_j(M) = \{i \in \{0, \dots, r_j - 1\} \mid H_M(j, i) \neq 0\}$. Now put $\omega_j(M) = \max\{\bar{\delta}(\mathbb{Z}_{r_j} \setminus \text{supp}_j(M)) \mid \delta \in \mathbb{B}\}$ and $\epsilon_j(M) = \max\{\Delta_{\mathbb{B}}(H_M(j, k)) \mid k \in \text{supp}_j(M)\}$ and set $\Delta_j(M) = \omega_j(M) \cdot \epsilon_j(M)$.

Finally, define the **apparent distance of M with respect to \mathbb{B}** (or the \mathbb{B} -apparent distance) as:

$$\Delta_{\mathbb{B}}(M) = \max\{\Delta_j(M) \mid j \in \{1, \dots, s\}\}.$$

For example, by taking $\mathbb{B} = \{\delta_{BCH}\}$, $\Delta_{\mathbb{B}}(M)$ is the strong apparent distance in [2]. On the other hand, we note that condition (2) of Remark 7 not necessarily holds in two or more variables.

Before showing examples, we relate the apparent distance to weight of code-words. For each polynomial $f = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} \mathbf{X}^{\mathbf{i}}$, consider the hypermatrix of the coefficients of f , denoted by $M(f) = (a_{\mathbf{i}})_{\mathbf{i} \in I}$. For any $j \in \{0, \dots, s\}$, if we write $f = \sum_{k=0}^{r_j-1} f_{j,k} X_j^k$, where $f_{j,k} = f_k(\mathbf{X}_j)$ and $\mathbf{X}_j = X_1 \cdots X_{j-1} \cdot X_{j+1} \cdots X_s$, then $M(f_{j,k}) = H_M(j, k)$. This means that "fixed" the variable X_j in f , for each power k of X_j , the coefficient $f_{j,k}$ is a polynomial in \mathbf{X}_j , and $H_M(j, k)$ is the hypermatrix obtained from the coefficients of this $f_{j,k}$. Now we extend Proposition 8 to several variables.

Theorem 10 *Let $f \in \mathbb{L}(r_1, \dots, r_n)$ and $M(f)$ the hypermatrix of its coefficients. Fix any $\bar{\alpha} \in U$. Then $\Delta_{\mathbb{B}}(M(f)) \leq \omega(\varphi_{\bar{\alpha}, f}^{-1})$.*

Proof. The case $n = 1$ is Proposition 8. We prove the theorem for matrices. The general case follows directly by induction.

Set $\bar{\alpha} = (\alpha_1, \alpha_2)$ and write $f = \sum_{k=0}^{r_2-1} f_{2,k} X_2^k$. Then $H_M(2, k)$ is the vector of coefficients of $f_{2,k}$. Clearly, $\text{supp}_2(M) = \text{supp}(f_{2,k})$ and, for any $k \in \text{supp}_2(M)$, we have $\Delta_{\mathbb{B}}(H_M(2, k)) \geq 1$. Then, by Proposition 8, $\omega(\varphi_{\alpha_1, f_{2,k}}^{-1}) \geq 1$.

By the definition of discrete Fourier transform $|\overline{Z(f_{2,k})}| = \omega(\varphi_{\alpha_1, f_{2,k}}^{-1})$, hence there exists $t \in \mathbb{Z}_{r_1}$ (at least one) such that α_1^t is a non zero of $f_{2,k}$.

Set $g(X_2) = f(\alpha_1^t, X_2) = \sum_{k=0}^{r_2-1} f_k(\alpha_1^t) X_2^k$ and note that it is a non zero polynomial. Let $v(g)$ be the vector of coefficients of $g(X_2)$. Then $\text{supp}(v(g)) \subseteq \text{supp}_2(M)$ and so $\Delta_{\mathbb{B}}(v(g)) \geq \max\{\bar{\delta}(\mathbb{Z}_{r_2} \setminus \text{supp}_2(M)) \mid \delta \in \mathbb{B}\} = \omega_2(M)$.

As $|\overline{Z(g)}| = \omega(\varphi_{\alpha_2, g}^{-1}) \geq \Delta_{\mathbb{B}}(v(g))$ then $|\overline{Z(f)}| \geq \omega_2(M) \cdot \Delta_{\mathbb{B}}(H_M(2, k))$. Finally, as in the univariate case, it is clear that $|\overline{Z(f)}| = \omega(\varphi_{\bar{\alpha}, f}^{-1})$ and this completes the proof. ■

Example 11 *Set $n = 72 = 3 \times 24$ and $q = 5$. Fix $\alpha_1 \in U_3$ and $\alpha_2 \in U_{24}$ and consider the 5-orbits matrix M afforded by $D = Q(0, 0) \cup Q(0, 1) \cup Q(0, 2) \cup Q(0, 3) \cup Q(0, 6) \cup Q(0, 7) \cup Q(0, 9) \cup Q(1, 0) \cup Q(1, 1) \cup Q(1, 5) \cup Q(1, 6)$. Choose $\mathbb{B} = \{\delta_{HT}, \delta_{BS}\}$, where δ_{HT} is the Hartman-Tzeng bound in [15] (see [9]) and δ_{BS} is the Betti-Sala bound in [3]. One may check that $\text{supp}_1(M) = \{0, 1, 2\}$ and $\omega_1(M) = 1$. On the other hand, $\text{supp}_2(M) = \mathbb{Z}_{24} \setminus \{0, 1, 5, 6\}$ and $\omega_2(M) = 4$, by using δ_{HT} . Now $\Delta_{\mathbb{B}}(H_M(1, 0)) = 8$, by using δ_{BS} (see [3, Example 4.2]) which is the maximum, and hence $\epsilon_1(M) = 8$. Finally it is clear that $\epsilon_2(M) = 2$, so that $\Delta_1(M) = \Delta_2(M) = 8$. We conclude $\Delta_{\{\delta_{HT}, \delta_{BS}\}}(M) = 8$.*

The reader may check that $\Delta_{\delta_{HT}}(M) = 8$ too, because although $\Delta_1(M) = 6$ we get $\Delta_2(M) = 8$. Moreover, one may check that for $\mathbb{B} = \{\delta_{BCH}\}$ we get $\Delta_1(M) = 5$ and $\Delta_2(M) = 6$ (because $\omega_2(M) = 3$), hence $\Delta_{\mathbb{B}}(M) = 6$.

Example 12 Set $q = 2$, $n = 75 = 5 \times 15$ and let M be the q -orbits matrix afforded by $D = Q(0, 0) \cup Q(0, 3) \cup Q(0, 5) \cup Q(0, 7) \cup Q(1, 0) \cup Q(1, 2) \cup Q(1, 4)$. In this case, one may check that $\Delta_{\{\delta_{BCH}, \delta_{HT}\}}(M) = 8$.

5 Apparent distance of abelian codes

The following definition changes a little the usual way to present the notions of apparent distance in [6] and the strong apparent distance in [2] (see also [16]). We recall that \mathbb{B} denotes a set of ds-bounds, which are used to proceed a concrete computation of the apparent distances.

Definition 13 Let C be an abelian code in $\mathbb{F}_q(r_1, \dots, r_s)$. 1) The **apparent distance of C with respect to $\bar{\alpha} \in U$ and \mathbb{B}** (or the $(\mathbb{B}, \bar{\alpha})$ -apparent distance) is

$$\Delta_{\mathbb{B}, \bar{\alpha}}(C) = \min\{\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha}, c})) \mid c \in C\}.$$

2) The **apparent distance of C with respect to \mathbb{B}** is

$$\Delta_{\mathbb{B}}(C) = \max\{\Delta_{\mathbb{B}, \bar{\alpha}}(C) \mid \bar{\alpha} \in U\}.$$

The following result is consequence of Theorem 10.

Corollary 14 For any abelian code C in $\mathbb{F}_q(r_1, \dots, r_s)$ and any \mathbb{B} as above, $\Delta_{\mathbb{B}}(C) \leq d(C)$.

Proof. Let $g \in C$ such that $\omega(g) = d(C)$. By Theorem 10, $\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha}, g})) \leq \omega(g)$ for any $\bar{\alpha} \in U$. From this the result follows directly. ■

It is certain that to compute the apparent distance for each element of a code in order to obtain the apparent distance of the code can be as hard work as to compute the minimum distance of such a code. Hence, to improve the efficiency of the computation the following result tells us that we may restrict our attention to the idempotents of the code. It also allows us to reformulate Definition 13 as it is presented in the mentioned papers.

Proposition 15 Let C be an abelian code in $\mathbb{F}_q(r_1, \dots, r_s)$. The apparent distance of C with respect to $\bar{\alpha} \in U$ and \mathbb{B} verifies the equality

$$\Delta_{\mathbb{B}, \bar{\alpha}}(C) = \min\{\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha}, e})) \mid e^2 = e \in C\}.$$

Proof. Consider any $c \in C$. Since $\mathbb{F}_q(r_1, \dots, r_s)$ is semisimple, then there exists an idempotent $e \in C$ such that the ideals generated by c and e in $\mathbb{F}_q(r_1, \dots, r_s)$ coincide; that is, $(c) = (e)$, and so, $\mathcal{D}_{\bar{\alpha}}(c) = \mathcal{D}_{\bar{\alpha}}(e)$. This means that $\text{supp}(M(\varphi_{\bar{\alpha}, c})) = \text{supp}(M(\varphi_{\bar{\alpha}, e}))$. Now, one may see that the computation of the apparent distance is based on the fact that the entries (of the matrices) are zero or not; that is, once an entry is non zero, its specific value is irrelevant.

Considering this fact, it is easy to see that $\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},c})) = \Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},e}))$ and so we get the desired equality. ■

If $e \in \mathbb{F}_q(r_1, \dots, r_s)$ is an idempotent and E is the ideal generated by e then $\varphi_{\bar{\alpha},e} \star \varphi_{\bar{\alpha},e} = \varphi_{\bar{\alpha},e}$, for any $\bar{\alpha} \in U$. Thus if $\varphi_{\bar{\alpha},e} = \sum_{\mathbf{i} \in I} a_{\mathbf{i}} X^{\mathbf{i}}$, we have $a_{\mathbf{i}} \in \{1, 0\} \subseteq \mathbb{F}_q$ and $a_{\mathbf{i}} = 0$ if and only if $\mathbf{i} \in \mathcal{D}_{\bar{\alpha}}(E)$. Hence $M(\varphi_{\bar{\alpha},e}) = M(\mathcal{D}_{\bar{\alpha}}(E))$. Conversely, let M be a hypermatrix afforded by a set D which is a union of q -orbits. We know that D determines a unique ideal C in $\mathbb{F}_q(r_1, \dots, r_s)$ such that $\mathcal{D}_{\bar{\alpha}}(C) = D$. Let $e \in C$ be its generating idempotent. One may verify that $M(\varphi_{\bar{\alpha},e}) = M(D)$.

Now let C be an abelian code, $\bar{\alpha} \in U$ and let M be the hypermatrix afforded by $\mathcal{D}_{\bar{\alpha}}(C)$. For any q -orbits hypermatrix $P \leq M$ [see the ordering (1)] there exists a unique idempotent $e' \in C$ such that $P = M(\varphi_{\bar{\alpha},e'})$ and for any codeword $f \in C$ there is a unique idempotent $e(f)$ such that $\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},f})) = \Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},e(f)}))$. So

$$\begin{aligned} \min\{\Delta_{\mathbb{B}}(P) \mid 0 \neq P \leq M\} = \\ \min\{\Delta_{\mathbb{B}}(M(\varphi_{\bar{\alpha},e})) \mid 0 \neq e^2 = e \in C\} = \Delta_{\mathbb{B}}(C). \end{aligned}$$

This fact drives us to give the following definition.

Definition 16 For a q -orbits hypermatrix M , its *minimum \mathbb{B} -apparent distance* is

$$\mathbb{B}\text{-mad}(M) = \min\{\Delta_{\mathbb{B}}(P) \mid 0 \neq P \leq M\}.$$

Finally, in the next theorem we set the relationship between the apparent distance of an abelian code and the minimum apparent distance of hypermatrices.

Theorem 17 Let C be an abelian code in $\mathbb{F}_q(r_1, \dots, r_s)$ and let e be its generating idempotent. For any $\bar{\alpha} \in U$ we have $\Delta_{\mathbb{B},\bar{\alpha}}(C) = \mathbb{B}\text{-mad}(M(\varphi_{\bar{\alpha},e}))$. Therefore, $\Delta_{\mathbb{B}}(C) = \max\{\mathbb{B}\text{-mad}(M(\varphi_{\bar{\alpha},e})) \mid \bar{\alpha} \in U\}$.

Proof. It follows directly from the preceding paragraphs. ■

6 Computing minimum apparent distance

In [2] it is presented an algorithm to find, for any abelian code, a list of matrices representing some of its idempotents (or hypermatrices in case of more than 2 variables) whose apparent distance based on the BCH bound (called the strong apparent distance) goes decreasing until the minimum value is reached. It is a kind of “suitable idempotents chase through hypermatrices” [2, p. 2]. This algorithm is based on certain manipulation of the hypermatrix afforded by the defining set of the abelian code. It is not so hard to see that it is possible to obtain an analogous algorithm in our case.

We reproduce here the result and algorithm in the case of two variables under our notation. Then we will use the mentioned algorithm to improve the searching of new bounds for abelian codes.

Definition 18 *With the notation of the previous section, let D be a union of q -orbits and $M = M(D)$ the hypermatrix afforded by D . We say that $H_M(j, k)$ is an **involved hypercolumn (row or column for two variables) in the computation of $\Delta_{\mathbb{B}}(M)$** , if $\Delta_{\mathbb{B}}(H_M(j, k)) = \epsilon_j(M)$ and $\Delta_j(M) = \Delta_{\mathbb{B}}(M)$.*

We denote the set of indices of involved hypercolumns by $I_p(M)$. Note that the involved hypercolumns are those which contribute in the computation of the \mathbb{B} -apparent distance.

The next result shows a sufficient condition to get at once the minimum \mathbb{B} -apparent distance of a hypermatrix.

Proposition 19 *With the notation as above, let D be a union of q -orbits and $M = M(D)$ the hypermatrix afforded by D . If $\Delta_{\mathbb{B}}(H_M(j, k)) = 1$, for some $H_M(j, k) \in I_p(M)$, then $\mathbb{B}\text{-mad}(M) = \Delta_{\mathbb{B}}(M)$.*

Proof. It is a modification of that in [2, Proposition 23] having in mind the use of different ds-bounds. ■

Theorem 20 *Let \mathcal{Q} be the set of all q -orbits modulo (r_1, r_2) , $\mu \in \{1, \dots, |\mathcal{Q}|-1\}$ and $\{Q_j\}_{j=1}^{\mu}$ a subset of \mathcal{Q} . Set $D = \cup_{j=1}^{\mu} Q_j$ and $M = M(D)$. Then there exist two sequences: the first one is formed by nonzero q -orbits matrices, $M = M_0 > \dots > M_l \neq 0$ and the second one is formed by positive integers $m_0 \geq \dots \geq m_l$, with $l \leq \mu$ and $m_i \leq \Delta_{\mathbb{B}}(M_i)$, verifying the following property:*

If P is a q -orbits matrix such that $0 \neq P \leq M$, then $\Delta_{\mathbb{B}}(P) \geq m_l$ and if $\Delta_{\mathbb{B}}(P) < m_{i-1}$ then $P \leq M_i$, where $0 < i \leq l$.

Moreover, if $l' \in \{0, \dots, l\}$ is the first element satisfying $m_{l'} = m_l$ then $\Delta_{\mathbb{B}}(M_{l'}) = \mathbb{B}\text{-mad}(M)$.

Proof. It follows the same lines of that in [2, Proposition 25] having in mind the use of different ds-bounds. ■

Algorithm for matrices.

Set $I = \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2}$. Consider the matrix $M = (a_{ij})_{(i,j) \in I}$ and a set \mathbb{B} of ds-bounds.

Step 1. Compute the apparent distance of M with respect to \mathbb{B} and set $m_0 = \Delta_{\mathbb{B}}(M)$.

Step 2.

- a) If there exists $H_M(j, k) \in Ip(M)$ (see Definition 18) such that $\Delta_{\mathbb{B}}(H_M(j, k)) = 1$ then we finish giving the sequences $M = M_0$ and $m_0 = \Delta_{\mathbb{B}}(M)$ (because of Proposition 19).
- b) If $\Delta_{\mathbb{B}}(H_M(j, k)) \neq 1$ for all $H_M(k, b) \in Ip(M)$, we set

$$S = \bigcup_{H_M(k, b) \in Ip(M)} \text{supp}(H_M(k, b))$$

and construct the matrix $M_1 = (a_{ij})_{(i, j) \in I}$ such that

$$a_{ij} = \begin{cases} 0 & \text{if } (i, j) \in \cup \{Q(k, b) \mid (k, b) \in S\} \\ m_{ij} & \text{otherwise.} \end{cases}$$

(In other words, $M_1 < M$ is the matrix with maximum support such that its involved rows and columns are zero. One may prove that if $0 \neq P < M$ and $\Delta_{\mathbb{B}}(P) < m_0$ then $P \leq M_1$.)

Step 3.

- a) If $M_1 = 0$ then we finish giving the sequences $M = M_0$ and $m_0 = \Delta_{\mathbb{B}}(M)$.
- b) If $M_1 \neq 0$, we set $m_1 = \min\{m_0, \Delta_{\mathbb{B}}(M_1)\}$, and we get the sequences $M = M_0 > M_1$ and $m_0 \geq m_1$. Then, we go back to Step 1 with M_1 in the place of M and m_1 in the place of m_0 . ■

Remark 21 *If the matrix has μ q -orbits the algorithm has at most μ steps. ■*

7 Examples

Example 22 *We take the setting of Example 11 and consider the abelian code C with $\mathcal{D}(C) = D$. In this case, the matrix $M = M(\mathcal{D}(C))$ is the same as that in the mentioned example. Choose again $\mathbb{B} = \{\delta_{HT}, \delta_{BS}\}$.*

By Example 11, $m_0 = 8$. Now $Ip(M) = \{H_M(1, 0)\} \cup \{H_M(2, j) \mid j \in \{2, 3, 7, 9, 10, 11, 15, 21\}\}$. One may check that $\Delta_{\mathbb{B}}(M_1) = \Delta_1(M_1) = \Delta_2(M_1) = 16$. Finally, as $\{H_M(1, 1), H_M(1, 2)\} \subset Ip(M_1)$ then $M_2 = 0$.

This code has $\dim_{\mathbb{F}_5}(C) = 52$ and $\Delta_{\mathbb{B}}(C) = 8$. The closer code we know is a $(105, 51, 7)$ binary cyclic code in [8, Table II]. The known bounds of linear codes are between 10-15.

Example 23 *Consider the abelian code related with the matrix in Example 12. So $q = 2$, $n = 75 = 5 \times 15$. Let C be the abelian code with defining set $\mathcal{D}(C) = D$, and choose, as in the mentioned example, $\mathbb{B} = \{\delta_{BCH}, \delta_{HT}\}$. In this case, $\Delta_{\mathbb{B}}(M_0) = 8$, $\Delta_{\mathbb{B}}(M_1) = 8$ and $\Delta_{\mathbb{B}}(M_2) = 15$.*

This code has $\dim_{\mathbb{F}_2} C = 52$ and $\Delta_{\mathbb{B}}(C) = 8$. It has the largest known bound to the minimum distance among the linear codes with the same length and dimension (see [5, p. 670] or [7]).

Table 1: Binary abelian codes with $n = 3 \times r_2$ and big rate

Code	n	dim	$\mathcal{D}(C)$ representatives	\mathbb{B}	Δ
C_1	21	16	$(0, 1), (1, 0)$	δ_{BCH}	3
C_2	45	39	$(0, 1), (1, 0)$	δ_{BCH}	3
C_3	51	35	$(0, 1), (1, 3)$	δ_{HT}	3
C_4	69	46	$(0, 0), (1, 1)$	$\delta_{SB}, \delta_{BCH}$	6
C_5	105	93	$(0, 5), (0, 7), (0, 15), (1, 0)$	$\delta_{HT}, \delta_{BCH}$	8

In Table 1 we include binary abelian codes of lengths $n = 3 \times r_2$ that may be of interest. The codes C_1 , C_2 and C_5 have the largest known bound to the minimum distance among the *linear codes* with the same length and dimension (see [5] or [7]). The codes C_3 and C_4 have a bound larger than that of any cyclic code with the same length and dimension (see [20]). The “shifting bound”, denoted δ_{SB} , is considered for the code C_4 (see [18, Example 7]). The reader may compare this codes with those in [21] and [12].

8 Conclusion

We have developed a technique to extend any ds-bound for cyclic codes to multivariate codes which can be applied to codes of arbitrary length, mainly for those whose minimum distance is still unknown. We use this technique to improve the searching of new bounds for abelian codes.

References

- [1] J.J. Bernal, J.J. Simón, *Partial permutation decoding for abelian codes*. IEEE Transactions on Information Theory **59** (8) (2013) 5152-5170.
- [2] J.J. Bernal, D.H. Bueno-Carreño, J.J. Simón, *Apparent distance and a notion of BCH multivariate codes*. IEEE Transactions on Information Theory, **62**(2), 2016, 655-668.
- [3] E. Betti, M. Sala, *A new bound for the minimum distance of a cyclic code from its defining set*. IEEE Transactions on Information Theory **52** (8) (2006) 3700-3706.
- [4] R.E. Blahut, *Decoding of cyclic codes and codes on curves*. In W.C. Huffman and V. Pless (Eds.), *Handbook of Coding Theory*, Vol. II, 1569-1633, 1998.

- [5] A. E. Brouwer, T. Verhoeff, An updated table of the minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 662–677, 1993.
- [6] P. Camion, *Abelian Codes*. MCR Tech. Sum. Rep. 1059, University of Wisconsin, Madison, 1970.
- [7] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes." Online available at <http://www.codetables.de>.
- [8] C.R.P. Hartmann, H. Tai-Yang, *Some results on the weight structure of cyclic codes of composite length*. *IEEE Transactions on Information Theory* **IT-22** (3) (1976) 340-348.
- [9] C.R.P. Hartmann, K.K. Tzeng, *Generalizations of the BCH bound*. *Information and Control* **20** (1972) 489-498.
- [10] H. Imai, *A theory of two-dimensional cyclic codes*. *Information and Control* **34**(1) (1977) 1-21.
- [11] T. Kaida, J. Zhen, *A decoding method up to the Hartmann-Tzeng bound using the DFT for cyclic codes*. In *Proceedings of Asia-Pacific Conference on Communications* (2007) 409-412.
- [12] J.M. Jensen, *The Concatenated Structure of Cyclic and Abelian Codes*. *IEEE Transactions on Information Theory* **IT-31**(6) (1985) 788-793.
- [13] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Elsevier, Amsterdam, 1977.
- [14] C. Roos, *A new lower bound for the minimum distance of a cyclic codes*. *IEEE Transactions on Information Theory* **29**(3) (1983) 330-332.
- [15] C. Roos, *A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound*. *J. Combinatorial Theory, Series A* (1982) 229-232.
- [16] R.E. Sabin, *On minimum distance bounds for Abelian Codes*. *Applicable Algebra Eng. Commun. Comput.* **3**(3) (1992) 183-197.
- [17] S. Sakata, *Decoding binary cyclic 2-D codes by the 2-D Berlekamp-Massey algorithm*. *IEEE Transactions on Information Theory* **37**(4) (1991) 1200-1203.
- [18] J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes*. *IEEE Transactions on Information Theory* **32**(1) (1986) 23-40.
- [19] K.-C. Yamada, *Hypermatrix and its applications*. *Hitotsubashi J. Arts Sciences* **6**(1) (1965) 34-44.
- [20] A. Zeh, T. Jerkovits. *Cyclic Codes* Online available at <http://www.boundtables.org>

- [21] J. Zhen, T. Kaida, *The designed minimum distance of medium length for binary cyclic codes*. ISITA-2012, Honolulu, Hawaii (2012) 441-445.